INFORMATION PAPER

NETC-EST-IA
22 May 2006

SUBJECT: Contractor Verification System (CVS) Implementation Guidance

1. Purpose. Outline the requirements to meet the 31 Jul 06 CVS implementation deadline. This task will require the concentrated effort of all Commanders, Directors of Security and Common Access Card (CAC) issuance personnel and the Administrative Contracting Community.

2. Background.

a. In Oct 00, DoD began to use the Real-Time Automated Personnel Identification System (RAPIDS) to produce the CAC as the standard form of identification for Active Duty, Selected Reserve, DoD Civil Servants, and eligible contractor personnel.

b. CAC issuance to the appropriate contractor personnel is required to access DoD buildings, computer networks, and other infrastructure. DoD policy dictates that an authorizing official (usually the Contracting Officer Representative (COR), Quality Assurance Evaluator (QAE), Contracting Officer Technical Representative (COTR), the designated contracting officer (KO) assigned to the installation contracting office, or the installation's designated representative sponsor the contractor and approve issuance of the CAC. This approval, which has previously been verified through the use of a DD 1172-2, form will now be verified through CVS.

3. Discussion.

a. The current manual processes supporting the application and approval for CAC issuance is vulnerable to exploitation and is prone to data inaccuracy among other identified shortcomings. To address deficiencies inherent in the current process of validating contractor CAC eligibility and subsequent manual entry into DEERS, USD (P&R) has directed the "lock down" of the DEERS data base to all but official sources of automated data. Consequently, as of 31 Jul 06, the Defense Manpower Data Center (DMDC) will disable the ability of a RAPIDS Verifying Official (VO) to manually add contractor data into DEERS thus mandating the utilization of CVS as the official authoritative data source.

b. Contractors requiring logical access to DoD computer systems and networks are mandated by DoD policy to utilize Public Key Infrastructure (PKI) certificates resident on the CAC. Once the DEERS lock down occurs, CACs may not be issued to contractors unless a data record authorizing CAC issuance is resident in DEERS. At present, there is no recognized Army data base of contractors that will facilitate this action. CVS was developed as a secure and authorized means of entering contractor data into the DEERS data base in addition to automating the CAC application and approval process.

c. HSPD-12, 14 Jan 06, mandates the establishment of secure and reliable forms of personal identification for all Federal civilian employees and contractors. It is anticipated that by Oct 06, all contractors will require issuance of a Personal Identity Verification (PIV) compliant credential, the CAC, for both logical and physical access.

d. Contractor information in the DEERS database can be made available to the Services as a resource to establish corporate level databases facilitating top level management actions such as analytical and statistical analysis as well as providing the basis for worldwide contractor accountability.

4. CVS Overview.

a. CVS is a web based application hosted on a DMDC server that allows for updating DEERS with DoD Contractor personnel data. CVS relies on an SSL capable internet browser for all users. For users authenticating to CVS with a CAC, a smartcard reader and middleware are also required on the client workstation.

b. CVS updates the DEERS Person Data Repository (PDR) with DoD Contractor data and utilizes the DEERS Security Online Website of the PDR to authenticate Trusted Agent Security Managers (TASM) and Trusted Agents (TA) as valid CVS users. It is necessary for an installation to obtain a site ID and identify an Installation POC prior to the commencement of CVS operations.

5. CVS Roles and Responsibilities: CVS implementation Army-wide will require establishment of the following roles, with the indicated requirements and responsibilities.

a. The Department of the Army Point of Contact (APOC) will serve as the primary interface to DMDC. The APOC, who is required to be Active Duty Military or a DA Civil Servant, must be preexistent in DEERS, and have a CAC.

b. Installation Point of Contact (IPOC) will serve as the primary interface to the APOC. The IPOC is required to be an Army Military or a DA Civil Servant, be preexistent in DEERS, and have a CAC.

c. Trusted Agent Security Manager (TASM) will be associated with a single CVS Program Site ID—an organization for which he/she is responsible. The TASM, who is required to be Army Military or a DA Civil Servant, must preexist in DEERS, and have a CAC.

d. Trusted Agent (TA) is required to be Army Military or a DA Civil Servant, must preexist in the DEERS, and have a CAC.

e. Contractor Company Representative (CCR) – An optional role that may be added to the CVS organization if it provides a value add to the associated business practice.

The Contractor Company Representative serves as his/her company's single point of contact to the appropriate TA.

f. DA Contractor Employee will contact the appropriate TA with the required information to initiate his/her request for a CAC.

6. Contractor Eligibility.

a. Contractor Employee – An employee of a firm, or individual under contract or subcontract to the DA, designated as providing services or support to the Department who requires physical and/or logical access to the facilities and/or systems.

b. Contingency Contractor Employee - An employee of a firm, or individual under contract or subcontract to the DA, designated as providing services or support vital to contingency, mobilization, or wartime missions. A contingency contractor employee must be located overseas or be subject to deployment overseas to perform functions in direct support of essential contractor service.

c. Personnel under contract who require physical access to a single DoD controlled facility will be issued a DBIDS (Defense Biometric Identification System) credential and will not normally receive a CAC. Where regional DBIDS is available, DBIDS will be used for contractors who require physical access only to DoD facilities within that region.

7. Background Vetting. The Joint Personnel Adjudication System (JPAS) is the authoritative source for background vetting. Beginning in 2006, a recurring data feed will be provided to DEERS/RAPIDS for identity vetting information this information will be used to determine if a credential can be issued.

8. Personnel eligible for a CAC who are not in JPAS (i.e., certain contractors, Foreign Nationals, and DoD affiliates) will be required to register at a site where an equivalent background vetting will be accomplished in accordance with FIPS 201, will be processed.

9. Re-verification.

a. CVS periodically generates a list of contractors requiring re-verification.

b. CVS obtains the current e-mail address for the sponsoring TA as recorded in the DEERS database.

c. CVS generates and sends an e-mail to the sponsoring TA with summary information indicating that contractors require re-verification.

d. The TA logs into the CVS web site with their CAC and reviews the list of contractors requiring re-verification.

e. The TA either approves or denies continued use of the CAC for each contractor.

f. If denied, the CVS updates DEERS which then notifies the Certificate Authority (CA) to revoke the digital certificates during the bulk revocation process. (CVS also notifies the contractor via e-mail that their CAC has been revoked. The sponsoring TA is responsible for collecting the contractor's CAC and returning it to the RAPIDS Site Security Manager (SSM).)

g. If the sponsoring TA does not review contractor information in a reasonable time frame, the system notifies the contractor via e-mail that they require re-verification. The contractor is then responsible for contacting the sponsoring TA or finding a new sponsoring TA to request re-verification.

h. If a contractor is not re-verified in a reasonable time frame, the system will automatically revoke the contractor's CAC, update DEERS, and revoke the certificates.

10. Re-issuance. A CAC will be replaced when lost or stolen, when printed information requires changes, or when any of the media (to include printed data, magnetic stripe, bar codes, chip or contactless chip) becomes illegible or inoperable. When a card is reissued, a re-verification of identity documentation is necessary to receive a new card. Three years after initial CAC issuance, the National Agency Check with Inquiries must be completed and reflected in JPAS.

11. Return of CAC Cards. Invalid, inaccurate, inoperative, or expired CACs shall be returned to a RAPIDS site for disposition. CACs may not be retained for personal reasons upon expiration or when DA affiliation of the employee has been terminated.

12. The assertive execution of this guidance is essential in securing the Army's badge issuance process for contractor personnel.

13. The point of contact for this Information Paper is the NETCOM PKI Help Desk, email: iacacpki.helpdesk@us.army.mil, telephone: 866-738-3222.

Susan Maks/ NETC-EST-IA/703-602-4006
Approved by COL Stephen J. Jurinko